

What is claimed is:

1 1. A method comprising:
2 receiving registration information from a user;
3 verifying the registration information;
4 issuing a digital credential to the user based upon a
5 result from the verification; and
6 communicating the registration information to a
7 central authentication service.

1 2. The method of claim 1 further including periodically
2 communicating a registration status of the user to the
3 central authentication service.

1 3. The method of claim 1 further including uploading
2 client software to the user's computer, wherein the client
3 software forces real-time authentication of the digital
4 credential using the central authentication service.

1 4. The method of claim 1 further including generating a
2 confirmation level for the digital certificate based on
3 the verification of the registration information.

005260: 6TE92960

1 5. The method of claim 1, wherein verifying the
2 registration information includes verifying a medical
3 license number.

1 6. A method comprising:
2 receiving a digital credential from a relying party,
3 wherein the digital credential is associated with a user
4 registered with a registration authority;
5 verifying an identity of the user based on the
6 digital credential;
7 verifying a registration status of the user with the
8 registration authority; and
9 authenticating the digital credential based on the
10 verifications.

1 7. The method of claim 6, wherein verifying the
2 registration status of the user includes accessing a local
3 copy of registration information maintained by the
4 registration authority.

1 8. The method of claim 6, wherein verifying the
2 registration status of the user includes querying the
3 registration authority.

006260-67E92960

1 9. The method of claim 6, wherein verifying the
2 registration status includes verifying that a medical
3 license for the user remains valid.

1 10. The method of claim 6, wherein verifying the identity
2 of the user includes using a public key for the
3 registration authority to verify a digital signature of
4 the digital credential.

1 11. The method of claim 6 further including reporting a
2 result of the verification to the relying party.

1 12. The method of claim 6 further including storing a
2 result of the verification in an activity log.

1 13. A method comprising:
2 initiating a challenge-response sequence from a
3 client computer when a user uses a digital credential;
4 receiving a challenge from a remote server; and
5 responding to the challenge using the digital
6 credential.

1 14. The method of claim 13 further comprising accessing a
2 registration authority to receive the digital credential.

006260-67E92960

1 15. The method of claim 13 further comprising forwarding
2 the digital credential to a central authentication service
3 in response to the challenge received from the remote
4 server.

1 16. A computing system comprising:
2 a web browser configured to accesses a remote server;
3 and
4 a plug-in software module executed by the web browser
5 to cause the server to perform a challenge-response
6 sequence when a user uses a digital credential.

1 17. The computing system of claim 16, wherein the plug-in
2 comprises a Java applet.

1 18. A method comprising:
2 forming a contract with a relying party to centrally
3 authenticate digital credentials issued by a registration
4 authority; and
5 charging the relying party for the authentication.

006260-6T92960

1 19. The method of claim 18, wherein charging the relying
2 party includes charging the relying party a subscription
3 fee.

1 20. The method of claim 18, wherein charging the relying
2 party includes charging the relying party a transaction
3 fee per authentication.

1 21. The method of claim 18, further comprising
2 authenticating a digital credential by:
3 verifying an identity of a user based on the digital
4 credential; and
5 verifying a registration status of the user with the
6 registration authority.

1 22. The method of claim 18 further comprising requiring
2 in the contract that the relying party digitally sign
3 communications presented to a user associated with the
4 digital credential.

1 23. A method comprising:
2 digitally signing an electronic input form; and
3 communicating the form to a user for completion.

0066260-5T E92960

1 24. The method of claim 23 further comprising:
2 receiving the completed form and a digital credential
3 associated with the user; and
4 forwarding the digital credential and the signed
5 input form to a central authentication service.

1 25. A system comprising:
2 a database configured to store registration
3 information received from a registration authority; and
4 an authentication server configured to verify a
5 digital credential according to the registration
6 information.

1 26. The system of claim 25, wherein the authentication
2 server is configured to receive the digital credential
3 from a relying party.

1 27. The system of claim 25, wherein the authentication
2 server is configured to:
3 verify an identity of a user based on the digital
4 credential;
5 verify a registration status of the user with the
6 registration authority; and

006260"6TE92960

7 authenticate the digital credential based on the
8 verifications.

1 28. An article comprising a computer-readable medium
2 having computer-executable instructions stored thereon for
3 causing a computer to:

4 receive a digital credential from a relying party,
5 wherein the digital credential is associated with a user
6 registered with a registration authority;

7 verify an identity of the user based on the digital
8 credential;

9 verify a registration status of the user with the
10 registration authority; and

11 authenticate the digital credential based on the
12 verifications.

1 29. The article of claim 28, wherein the instructions
2 cause the computer to access a local copy of registration
3 information maintained by the registration authority.

1 30. The article of claim 28, wherein the instructions
2 cause the computer to query the registration authority.

006260-6792960

1 31. The article of claim 28, wherein the instructions
2 cause the computer to verify that a medical license for
3 the user remains valid.

1 32. The article of claim 28, wherein the instructions
2 cause the computer to use a public key for the
3 registration authority to verify a digital signature of
4 the digital credential.

1 33. A method comprising:
2 receiving a challenge signed by a digital credential
3 from a relying party, wherein the digital credential is
4 associated with a user registered with a registration
5 authority;
6 verifying an identity of the user based on the
7 digital credential;
8 verifying a registration status of the user with the
9 registration authority; and
10 authenticating the user for the relying party based
11 on the verification.

1 34. A method comprising:
2 issuing a digital credential to a user; and

006260.57E92960

3 verifying all uses of the digital credential at a
4 central authentication service.

1 35. The method of claim 34, further comprising recording
2 uses of the digital credential at the central
3 authentication service.

1 36. The method of claim 35, further comprising receiving
2 a request from a relying party for verification of the
3 digital credential, and communicating the result of the
4 verification to the relying party.

1 37. The method of claim 36, wherein the relying party is
2 one of a plurality of relying parties.

1 38. A method comprising:
2 receiving information from a registration authority;
3 and
4 creating a digital credential for a user based on the
5 information received from a registration authority,
6 wherein the information includes both substantially
7 static and substantially dynamic information.

006260-6T E92960

1 39. The method of claim 38, wherein the static
2 information includes registration information, and the
3 dynamic information includes good standing information.

1 40. The method of claim 38, further comprising updating
2 the dynamic information on a substantially regular basis.

1 41. The method of claim 38, further comprising recording
2 one or more biometric characteristics for the user.

006260 STE92960